

[ABOUT US \(HTTP://MACKENZIEINSTITUTE.COM/ABOUT-US/\)](http://mackenzieinstitute.com/about-us/)

[INSTITUTE NEWS \(HTTP://MACKENZIEINSTITUTE.COM/CATEGORY/INSTITUTE-NEWS/\)](http://mackenzieinstitute.com/category/institute-news/)

[EVENTS \(HTTP://MACKENZIEINSTITUTE.COM/CATEGORY/EVENTS/\)](http://mackenzieinstitute.com/category/events/)

[CALL FOR WRITERS \(HTTP://MACKENZIEINSTITUTE.COM/CALL-FOR-WRITERS/\)](http://mackenzieinstitute.com/call-for-writers/)

[CONTACT US \(HTTP://MACKENZIEINSTITUTE.COM/CONTACT-US/\)](http://mackenzieinstitute.com/contact-us/)

[EMAIL SIGN-UP \(HTTP://MACKENZIEINSTITUTE.COM/EMAIL-SIGN-UP/\)](http://mackenzieinstitute.com/email-sign-up/)



[\(http://mackenzieinstitute.com/\)](http://mackenzieinstitute.com/)

http://mackenzieinstitute.com/wp-content/uploads/2016/12/MI-SECURITY-MATTERS_Volume-III-003.pdf

[\(http://mackenzieinstitute.com/help-support-mackenzie-institute/\)](http://mackenzieinstitute.com/help-support-mackenzie-institute/)

Events (<http://mackenzieinstitute.com/category/events/>), Institute News (<http://mackenzieinstitute.com/category/institute-news/>)

"Money-Laundering, Cryptocurrencies & Cyber-Security" Conference Overview



ALEXANDER SAWICKI ([HTTP://MACKENZIEINSTITUTE.COM/AUTHOR/ALEXSAWICKI/](http://mackenzieinstitute.com/author/alexstawicki/))

10/13/2017, 12:03 pm

Below is a synopsis of our "Money-Laundering, Cryptocurrencies & Cyber-Security" conference held on November 16, 2017 at the Albany Club in Toronto, Ontario, Canada.

The keynote presentation from Diane Francis, Editor-At-Large at the *National Post*, repeatedly reinforced the major theme that would permeate the conference throughout the entire day: Canada is behind the curve. She began by discussing the impact of the "Panama Papers" and the more recent "Paradise Papers," which revealed that many Canadians, not just the ultra-rich elites, were turning to offshore tax havens in order to avoid paying their fair share. The problem with this

is, aside from the immediate losses to income tax revenue, is that this trend is likely due to continue as a result of the current structure of Canadian tax law. Moreover, Ms. Francis asserted that Canada was itself being used as a tax haven by both foreigners and domestic business owners for the very same reason: Canadian tax law has yet to enter the 21st century and adapt to the ever-changing global landscape.

It is not just tax law that is in dire need of an overhaul, because the Canadian real-estate market has its own set of problems that require attention – and soon. According to Ms. Francis, Vancouver is now the third most expensive real estate market in the world. Why? Aside from speculators and ordinary people simply trying to find a place to live, the Chinese are desperate to get their money out of mainland China and are doing so by parking their money in the Canadian real estate market, all the while using intermediaries located right here in Canada to cover their tracks.

This is not an isolated problem. Toronto is also becoming a hub for money-laundering and tax evasion by foreign nationals looking to get their money out of their home countries, where the government or the mafia can seize their cash at any time. And again, they are using Toronto's real estate market, coupled with local intermediaries and Canadian privacy laws, to get their money out and cover their tracks in the process.

This has become such a problem in Toronto that it is not uncommon to hear about so-called "zombie buildings" – units that are owned yet sit unoccupied, purchased in batches of up to forty at a time, sight-unseen, and are regularly flipped by speculators and foreign nationals alike. This practice has spawned an entire industry in Toronto whose only output is yet more high-rise buildings, and yet more units that are destined to sit empty. As a consequence, housing costs in Canada have ballooned to the point where Canadians are now saddled with the highest consumer debt in the world, just to be able to have a roof over their heads. That's a tough pill to swallow, especially in today's economy.

On the cyber-security and cryptocurrency front, law enforcement professionals from the first panel described their own difficulties navigating existing Canadian laws to pursue charges against those using cyberspace for nefarious activities. Chief Superintendent John Sullivan of the Ontario Provincial Police (OPP), Detective Alpha Chan of the Toronto Police Service, and Peter Warrack, the head of investigations with the AML Financial Intelligence Unit at the Royal Bank of

Canada, each detailed their own concerns which circled the same drain: the Canadian legal system is ill-equipped to deal with the cyber-threats of the 21st century.

Chief Superintendent Sullivan was particularly focused on organized crime groups and their increasing reliance on cryptocurrencies for money-laundering purposes. He said that, real estate firms, financial trusts, and shell corporations are hiding behind Canadian privacy laws to purposefully obfuscate their clients and hinder or otherwise delay investigations by the OPP. And, coupled with the 2016 Supreme Court ruling in *R v. Jordan*, which set a limit on how long legal proceedings may take place, it is becoming a monumental task for investigators to build a strong enough case in sufficient time to account for the myriad of procedural delays introduced by defence lawyers.

Detective Chan echoed a similar sentiment. He too was frustrated by the shackles imposed upon him by the system within which he must operate. When it comes to reporting cyber-crime, businesses are hesitant to come forward for fear of bad publicity, and when they actually do, are reticent to disclose the full extent of the breach or provide much in the way of helpful information to police. There is also the problem of jurisdiction. How is one to report a crime, and to whom, if the perpetrator was acting from cyber-space, a global entity, against a multinational corporation? But, Detective Chan, emphasized, it goes still deeper than that. Even something that should be a relatively trivial matter, such as filling out a form documenting a seizure of ill-obtained goods or funds, is brought to its knees if the goods exist in the virtual realm, such as Bitcoins or any other of over 1,200 different flavours of cryptocurrencies currently in existence. Moreover, when it comes to prosecution, many judges are completely and utterly clueless when it comes to matters concerning cyberspace – and not through any fault of their own, as this is a systemic issue for which a legal precedent has not yet been set.

All is not lost however, as the second panel did their best to extoll the virtues of cryptocurrencies by listing how something like Bitcoin will ultimately benefit global commerce. Yet again, the panel drew attention to the need for governments to step in and formally regulate cryptocurrencies. Further, they stressed the importance of having legislators who know what they are dealing with; failure to heed this warning will collectively result in a decisive lack of action from lawmakers, or worse, the passing of legislation that is wholly inadequate and out of sync with contemporary needs. In the meantime, as pointed out by Cynthia Ayers, a candidate for the US Senate, terrorist groups and organized crime

syndicates around the world (who often work hand in glove) are more than happy to sit back and continue to use cryptocurrencies to conduct illicit transactions, while the rest of us wait patiently for a day of reckoning.

The third panel spent considerable time discussing aspects of the hidden part of the internet known as the "Dark Web," which is often associated with shady dealings and criminality. Dr. Eric Jardine, an assistant professor at Virginia Tech, shared some of the findings from his research, which was meant to explore the prevalence of cryptocurrency transactions over the Dark Web. He found that, in stark contrast to the general public's perceptions, cryptocurrencies were only actually used in 30 – 60 per cent of all transactions. Paul Hanley, Lead Cyber Partner for Deloitte, also shared some of his experiences dealing with the "Enigma Forum," which was based on the Dark Web. This group of individuals focused on hacking into employee devices at certain large corporations, with the intent of collecting scandalous information that could later be used to blackmail these employees into giving up passwords to company systems. Ostensibly, the hackers used a piece of malware called "Delilah," which tapped into webcams and microphones and recorded the target at all hours of the day.

Lastly, the fourth panel reflected on the nature of cyber-security, arguing that the need is omnipresent due to the speed with which attackers are able to innovate and adapt. Liz Shirley, Technical Director of Intelligence and Tech Analysis at Wapack Labs and Red Sky Alliance, reinforced the need for constant vigilance. She argued that it simply will not suffice to periodically patch or update systems; firms must take it upon themselves to do their due diligence and ensure that their entire supply chain is not only meeting, but exceeding baseline regulations and standards concerning cyber-security. To do less is to court disaster – it is not a question of "if" a breach will occur, but "when."

Facebook (<http://www.facebook.com/sharer/sharer.php?u=http://mackenzieinstitute.com/november-16-2017-money-laundering-cryptocurrencies-cyber-security-conference/&t=%22Money-Laundering%2C+Cryptocurrencies+%26+Cyber-Security%22+Conference+Overview>)

Twitter

Google+ (<https://plus.google.com/share?url=http://mackenzieinstitute.com/november-16-2017-money-laundering-cryptocurrencies-cyber-security-conference/>)

Pinterest

LinkedIn ([http://www.linkedin.com/shareArticle?](http://www.linkedin.com/shareArticle?mini=true&ro=true&trk=EasySocialShareButtons&title=%22Money-Laundering%2C+Cryptocurrencies+%26+Cyber-Security%22+Conference+Overview&url=http://mackenzieinstitute.com/november-16-2017-money-laundering-cryptocurrencies-cyber-security-conference/)

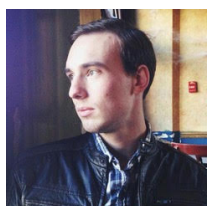
[mini=true&ro=true&trk=EasySocialShareButtons&title=%22Money-](http://www.linkedin.com/shareArticle?mini=true&ro=true&trk=EasySocialShareButtons&title=%22Money-Laundering%2C+Cryptocurrencies+%26+Cyber-Security%22+Conference+Overview&url=http://mackenzieinstitute.com/november-16-2017-money-laundering-cryptocurrencies-cyber-security-conference/)

[Laundering%2C+Cryptocurrencies+%26+Cyber-](http://www.linkedin.com/shareArticle?mini=true&ro=true&trk=EasySocialShareButtons&title=%22Money-Laundering%2C+Cryptocurrencies+%26+Cyber-Security%22+Conference+Overview&url=http://mackenzieinstitute.com/november-16-2017-money-laundering-cryptocurrencies-cyber-security-conference/)

[Security%22+Conference+Overview&url=http://mackenzieinstitute.com/november-16-2017-money-](http://www.linkedin.com/shareArticle?mini=true&ro=true&trk=EasySocialShareButtons&title=%22Money-Laundering%2C+Cryptocurrencies+%26+Cyber-Security%22+Conference+Overview&url=http://mackenzieinstitute.com/november-16-2017-money-laundering-cryptocurrencies-cyber-security-conference/)

[laundering-cryptocurrencies-cyber-security-conference/\)](http://www.linkedin.com/shareArticle?mini=true&ro=true&trk=EasySocialShareButtons&title=%22Money-Laundering%2C+Cryptocurrencies+%26+Cyber-Security%22+Conference+Overview&url=http://mackenzieinstitute.com/november-16-2017-money-laundering-cryptocurrencies-cyber-security-conference/)

#Canada #Canadian security #Cryptocurrencies #cyber #Cyber Security
#Money Laundering #Security



Alexander Sawicki

(<http://mackenzieinstitute.com/author/alexsawicki/>)

Alexander Sawicki is a freelance writer and IT consultant. Formerly a Research Analyst for the NATO Association of Canada, he graduated with an Honours Bachelor's Degree in History from Ryerson University in 2016, and throughout his university career has been deeply interested in international affairs.

Alexander also had the opportunity to work for the Canadian Border Services Agency (CBSA) as a Student Border Services Officer, and gained a wealth of firsthand experience defending the safety and security of Canadians. In the future, Alexander plans on pursuing a Master's Degree in the History of Science and Technology.